(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 165 789 B1**

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication of patent specification: **27.11.91** (51) Int. Cl.5: **G06F 1/00**

(21) Application number: **85304274.5**

(22) Date of filing: **14.06.85**

(54) Device for protecting computer software.

(30) Priority: **20.06.84 US 622657**

(43) Date of publication of application:
27.12.85 Bulletin 85/52

(45) Publication of the grant of the patent:
27.11.91 Bulletin 91/48

(84) Designated Contracting States:
BE DE FR GB IT

(56) References cited:
EP-A- 0 084 441
EP-A- 0 089 876
US-A- 3 806 882
US-A- 4 562 306

PATENT ABSTRACTS OF JAPAN, vol. 6, no. 183 (P-143)[1061], 18th September 1982; & JP-A-57 97 162 (FUJITSU K.K.) 16-06-1982

PATENT ABSTRACTS OF JAPAN, vol. 7, no. 180 (P-215)[1325], 9th August 1983; & JP-A-58 82 355 (HITACHI SEISAKUSHO K.K.) 17-05-1983

(73) Proprietor: **EFFECTIVE SECURITY SYSTEMS, INC.**
1701 West Civic Drive
Milwaukee Wisconsin 53209(US)

(72) Inventor: **Dunham, Michael D.**
2615 East Beverly Road
Shorewood Wisconsin 53211(US)
Inventor: **Vahlsing, Donald W.**
1725 Manchester Drive
Grafton Wisconsin 53024(US)
Inventor: **Dykstra, Thomas M.**
11029 North San Marino Drive 3W
Mequon Wisconsin 53092(US)
Inventor: **Ehlers, Paul L.**
232 Sunset Drive
Menasha Wisconsin 54952(US)

(74) Representative: **Skone James, Robert Edmund et al**
GILL JENNINGS & EVERY 53-64 Chancery Lane
London WC2A 1HN(GB)

EP 0 165 789 B1

ELECTRONIQUE INDUSTRIELLE, no. 73, 15th June 1984, pages 77-78, Paris, FR; J. BLADOU: "Accroissement de la protection logicielle par les micro-ordinateurs à EEPROM"

PATENT ABSTRACTS OF JAPAN, vol. 8, no. 60 (P-262)[1497], 22nd March 1984; & JP-A-58 208 861 (FUJITSU K.K.) 05-12-1983

PATENT ABSTRACTS OF JAPAN, vol. 8, no. 45 (P-257)[1482], 28th February 1984; & JP-A-58 195 975 (CANON K.K.) 15-11-1983

PATENT ABSTRACTS OF JAPAN, vol. 8, no. 141 (P-283)[1578], 30th June 1984; & JP-A-59 41 061 (FUJITSU K.K.) 07-03-1984

Description

This invention relates to an apparatus for monitoring the use of software in a computer system with respect to at least one selected aspect of such use, the computer system having a central processor containing the software, and the central processor being accessed by at least one operator terminal connected to it. More particularly, the invention relates to a combination software and hardware device for use with computer systems having one or more consoles or terminals connected to a central processing unit.

Computer software, programs, or packages of programs are often licensed by the developer or other supplier to the user or customer. The software licence may provide that, for a prescribed payment, the program may be used a given number of times, or for a given number of hours, or on a particular computer system, or on a given number of terminals. Licensing of software on a per terminal basis would be highly desirable as a convenient way to distinguish small users from large users and adjusting payments accordingly.

However, once the software is provided to the customer by the supplier, it is currently very difficult for the supplier thereafter to control the access, use, or transfer of the software. It is correspondingly difficult for the supplier to police the software licence. As a result, suppliers are often reluctant to enter into limited licences. The advantages of such licences, for example lower cost to small users or flexible pricing, are lost.

Techniques for the control or protection of computer programs currently use either a software approach or a hardware approach. A hardware approach to preventing unauthorised use of computer programs typically employs a physical key, such as a specially-coded card which must be inserted in a lock in the computer system before access can be had to the program. The key provides data, such as an electronic serial number or authorisation number. The correctness of the data must be properly verified before a program can be run. Alternatively, a programmable read-only memory (PROM) may be inserted in the computer system. The program then detects an authorisation number in the PROM to permit the program to operate. Another approach is to put authorisation data, such as a serial number, physically in the circuitry of the computer system. When the program is initially run, the authorisation data of the computer system are entered in a blank in the program. Thereafter, the program will only run if the authorisation data are present.

While the security provided to the program is high with the hardware approach, there are factors which limit its use. A major drawback is cost, both in the key and in the modification to the computer system. This has tended to limit the hardware approach to protection of large, expensive software programs. Many manufacturers do not put a serial number in the circuitry of the computer. Also, if the computer circuitry must be changed, there is a problem of getting the new authorisation data into the program. Further, the hardware approach is not particularly well suited for situations where use of the program is to be permitted, but under limited conditions.

In the software approach to program protection, the program is altered by encryption techniques so that it is not accessible without a software key placed on the medium containing the program, such as a computer disc. The software approach is less expensive than the hardware approach but less secure. Furthermore, there are several problems in the software approach. One is that it prevents legitimate copying as where an authorised user wishes to make a back-up copy of the program. A second drawback is that devices known as nibble copiers can duplicate all the software on the disc, including the software key, so that the security is greatly compromised. Nor does the software approach protect against an unauthorised taking of the program from one computer system to another, since the security data are transferred along with the program.

Because of the shortcomings of the hardware only and software only approaches, combined software and hardware techniques are becoming available. One such approach to the prevention of copying places a unique pattern or fingerprint on blank media, such as floppy discs, for storing the program. The program is placed on the disc by the manufacturer through software that encrypts the program source code several times to link the encrypted program to the unique pattern. The program can then be accessed only if the pattern is present, thus preventing copying of the program. However, this, and similar approaches, are limited to the media element of the computer system.

None of the foregoing techniques permit authorised use, whilst preventing use of the program or software outside limits authorised or established in a software licence.

US-A-3806882 describes a system that controls access to information stored in a computer by means of a portable electronic key device which either prevents or allows access to the computer.

JP-A-57-97162 relates to preventing access to a central data file. A terminal discriminating and processing part determines whether a requesting end user is an authorised user or not. Only authorised users are permitted access to the files, but once in have unlimited use.

JP-A-58-82355 prevents improper use of porta-

ble terminal equipment by registering information for preventing improper use, and its permitted frequency of error. When an error count of input data exceeds the previously registered permitted error frequency, the equipment is made ineffective.

The present invention is directed to a software-hardware device for controlling access to a main or host computer, and the programming contained therein, from one or more computer terminals or consoles. The access may be controlled in accordance within limits established in a software licence.

According to the invention there is provided apparatus for monitoring the use of software in a computer system with respect to at least one selected aspect of such use, the computer system having a central processor containing the software, the central processor being accessed by at least one operator terminal connected to the central processor; the apparatus comprising receiving means coupled to the central processor, memory means for containing data establishing the software usage limit for the selected aspect, microprocessor control means, and interrupt means; characterised in that the software in the central processor generates usage data indicative of monitored software usage for the selected aspect of the computer system, the apparatus employing at least one pre-established level of occurrences of conditions violating the usage limit for the selected aspect when monitoring use of the software; in that the receiving means is coupled to the central processor for receiving the monitored software usage data from software in the central processor; in that the memory means contains data establishing the pre-established level of occurrences of violating conditions, and stores violating condition occurrence data arising from operation of the computer system, and records data indicative of existing usage of the monitored software; in that the microprocessor control means is coupled to the receiving means and to the memory means for determining, in response to the usage data, the conditions violating said usage limit and for determining whether the occurrence of the violating conditions bears a predetermined relationship to the established level of occurrences of violating conditions; and in that the interrupt means is coupled to the computer system and to the control means, and is controlled by the control means to provide an output to the computer system when occurrences of violating conditions bear the predetermined relationship to the established level of occurrences of violating conditions, said output operating to control, in accordance with the relationship thus determined, the use of the software in the computer system in a predetermined manner.

In a typical application of the device, data not significant to security, for example data occurring during the ordinary operation of the computer system, pass unimpeded between the central processing unit and the terminal. When data having significance from the security standpoint are sent from a terminal to the central processing unit, the computer system will interrogate the security device of the present invention. Such data might typically be a request to run a particular program. The device has the use limits permitted by the software licence programmed into it. If the request is proper and within the limits established by the software licence, operation of the program is permitted. If the request is not proper, the security device produces a variety of consequences. For infrequent improper requests, operation of the program may be permitted, depending on the applications program, but with an appropriate warning displayed on the computer terminal. For frequent improper requests, operation of the program is blocked by the security device until released by the software owner or supervisory personnel.

The device of the present invention, which is independent of the central processing unit, thus monitors program access requests so as to properly control access to the programs in the central processing unit.

By contrast to other approaches to program security, the device of the present invention is an intelligent device having interactive capabilities. For this purpose, the device may employ a microprocessor. The device is readily auditable to ascertain which programs are authorised and the limits of that authorisation. The device may also store commercial data relating to the programs, such as the name of the software licensee. The authorisation can easily be changed in the field through a local terminal or through a remote terminal connected by a modem. Warning messages and the like provided by the device can be similarly changed.

The device may use units, such as cartridges, which can be inserted into the device to permit control of the authorisation of software application packages or supplier-designated software products, such as word processing or graphics programs. This provides increased authorisation control, maintainability, and field reliability. For instance, multiple software suppliers can control and maintain use of their products without coordination with other software suppliers in a single computer system. This is in contrast to past approaches in which a single knowledgeable source of the authorised configuration must be reached to restore operation of the computer system following the field failure.

Embodiments of the invention will now be described, by way of example, with reference to the accompanying drawings, in which

Fig. 1 is a schematic diagram showing a software protection device of the present invention in a computer system having a central processing unit and one or more terminals;

Fig. 2 is a schematic diagram showing an alternative connection of the software protection device in a computer system;

Fig. 3 is a schematic block diagram of a software protection device of the present invention connected, as shown in Fig. 1, to the central processing unit;

Figs. 4A and 4B form a flow chart showing operation of the software protection device;

Fig. 5 is a schematic block diagram showing details of the software protection device connected to a computer system in a manner alternative to Figs. 1 and 2;

Fig. 6 is a schematic diagram showing details of a software protection device of the present invention suitable for connection to the computer system as shown in Fig. 2; and

Fig. 7 is a schematic diagram showing use of a plurality of security devices of the present invention to increase the number of programs that can be protected.

Referring to Fig. 1, a software protection device 10 of the present invention may be interposed in a data signal link or line 12a and 12b between a computer terminal 14 and a central processing unit 16 of a computer system. Other terminals 14a, 14b may be connected to the central processing unit 16. For some types of central processing units, a second connection between the device 10 and the computer 16 may be made by a link or line 18 for security purposes because of the particular operating system used. The line 18 is connected to an additional peripheral port of the central processing unit 16. Alternatively, the device 10 may be connected to the central processing unit 16 only via the line 18, as shown in Fig. 2.

The internal configuration of the device 10 is shown in Fig. 3. The device 10 shown in Fig. 3 is suitable for the connection shown in Fig. 1. The data signal line 12a from the terminal 14 is coupled to a port 50 of the device 10. The data signal line 12b, connected to the data port of the central processing unit 16, is coupled to a data port 52 of the device 10. Internal lines 12' and 12" interconnect the ports 50 and 52 to maintain the data signal path between the terminal 14 and the central processing unit 16. The arrows shown in Fig. 3 symbolically show the flow of data to and from the central processing unit 16 and the terminal 14. The line 12" contains signal level shifters 54 and 56 which alter the signals in the line 12" to levels appropriate for the operation of device 10, central processing unit 16, and terminal 14. Level shifters 54 and 56 may comprise integrated circuit RS 232 level shifters, such as that made and sold by National Semiconductor Corp., under the model no. 1488 or 1489. Line 12" also includes an interrupt means 58, shown diagrammatically as a switch operable by controller 60. Interrupt means 58 may be operated by controller 60 to cause the display of warning messages on terminal 14 in certain operating modes of the device and to disable data signal lines 12a, 12b under certain conditions of attempted unauthorized use, as described below, from the standpoint of passing normal data traffic.

A second pair of internal data lines 18' and 18" are provided in device 10. Lines 18' and 18" are connected to port 62 and to security data line 18 leading to the additional peripheral port of central processing unit 16. The other ends of lines 18' and 18" may be connected to port 64 that permits additional security devices to be connected in series with the device shown in Fig. 3, as shown in Fig. 7. Data line 18' includes signal level shifters 66 and 68 similar to level shifters 54 and 56. Data line 18' also includes an interrupt means 70 operable by controller 60 to supply information and commands to the software program in central processing unit 16.

Universal asynchronous receiver-transmitter 72 has the receiver port connected through level shifter 74 to data line 18". The transmit port is connected to interrupt means 58 and 70. Receiver-transmitter 72 may comprise an integrated circuit, such as that made and sold by Signetics, as model no. SCN2651.

Controller 60 may be a microprocessor, such as that made and sold by the Motorola Corporation, of Phoenix, Arizona, under the designation MC6809. Watchdog 76 may comprise a monostable multivibrator that clocks and resynchronizes controller 60 to insure proper operation of controller 60.

Data bus 78 connects controller 60 to memory 80. Memory 80 may comprise an electronically erasable programmable read only memory (EEPROM). Universal asynchronous receiver transmitter 72 is connected to data bus 78.

Memory 80 contains data relating to the operating system for central processing unit 16. It may also contain the data maintenance and operating programs for device 10, as well as a map of the data contained in cartridges 82 hereinafter described.

Data relating to the programs authorized to run on the computer system 14-16 is contained in plug-in cartridges 82a, 82b, and 82c. These plug-in cartridges may each comprise an electronically erasable programmable read only memory (EEPROM) containing data specific to a particular vendor. The EEPROM contains the limits of authorization for the various programs and packages

contained in central processing unit 16. A map of the data in the cartridge is also included in the EEPROM. The cartridges are connected to controller 60 by data bus 84.

Device 10 operates as follows, as shown in flow chart form in Fig. 4. Device 10 monitors line 18 from the security port of central processing unit 16 as at step 100 in Fig. 4 to ascertain the presence of information significant to program security. Thus, when a request from terminal 14 to central processing unit 16, via the applications software program in central processing unit 16, requests authorization to run a particular program, the application software in central processing unit 16 will, in turn, issue a request in security lines 18 to device 10 as at step 102 to inquire whether running of the program is authorized. The request will be received by universal asynchronous receiver-transmitter 72 and provided to controller 60. Controller 60 through data bus 84 will interrogate the applicable cartridge 82 to obtain the authorization data relating to the requested program, as at step 104. If the request is within the authorization provided in the software license, controller 60 will provide a response through receiver-transmitter 72 in data bus 18', 18" to the associated port of central processing unit 16 indicating to the computer system that operation of the program is authorized. The program is then permitted to run. This is shown in Fig. 4 as step 106.

If the analysis of the request for program authorization at step 104 indicates that the request is not within authorized limits, the following operation will occur. The applicable cartridge 82 contains data relating to the number of unauthorized requests for the program; the time of the last unauthorized request; and a moving average of the frequency of unauthorized requests. This data is interrogated by controller 60 via data bus 84 at steps 107, 108, and 110 of Fig. 3. At the same time the stored data is updated at steps 112, 114, and 116. Computation of the moving average may employ an exponential smoothing function in which latter entries may be related to earlier entries in a desired manner to reflect the number of incidents of significance in the average.

Based on the frequency at which unauthorized requests are occurring, one of four events will occur in protective device 10. The frequency levels at which the various events will occur are programmed into cartridges 82 by the software supplier.

A very low frequency of unauthorized requests indicates that the unauthorized requests are probably occurring through inadvertency or genuine error. For example, a terminal operator may inadvertently request the wrong program. Or, the correct program may be requested but at the wrong time.

If the frequency of unauthorized request is less than some predetermined number A programmed into the applicable cartridge 82, as determined in step 118 of Fig. 4, an error message is sent to central processing unit 16 from protective device 10 at step 119 for whatever further action may be undertaken by the applications software. The message will be provided from receiver-transmitter 72, as controlled by controller 60, and interrupt device 70. The message indicates that a violation has occurred but that it is a low level violation. This may be termed a Level I violation. The applications software will typically provide a warning on the operator's terminal screen 14. Other typical action that could be taken by the application software might include entry in a master log in central processing unit 16 or the provision of a warning signal to a supervisory terminal connected to central processing unit 16. Normally the application software would be permitted to run after the appropriate warning signal has been recorded and/or given, as shown in Fig. 4. For infrequent violations, it will be appreciated that the operation of device 10 is basically open loop. Messages are sent to central processing unit 16 but no other action is taken by device 10.

If the unauthorized requests are occurring at a greater frequency, this may be taken as evidence that some deliberate attempt is being made to obtain unauthorized access to the programs in central processing unit 16. Step 120 in the flow chart of Fig. 4 ascertains that the frequency of unauthorized requests is greater than the threshold A of step 118 but less than some greater frequency B also programmed into the applicable cartridge 82. This may be termed a Level II violation. Under this circumstance, an error message is sent to the application software in central processing unit 16, as at step 121, similar to the action 119 taken for low frequency violations. However, additionally, a timer provided in controller 60 is set in operation as at step 123. If security device 10 does not receive an appropriate response from the software in central processing unit 16, within the time period of the timer as at step 125 receiver-transmitter 72 provides a signal in line 18 from interrupt device 70 to disable that particular piece of software from running in central processing unit 16 as at step 127. The computer system can run other software for which authorization is not required or for which authorization is properly obtained.

If the software in central processing unit does provide the appropriate response to protection device 10 within the time period of the timer, the software is permitted to run in the same manner as described in connection with step 118. The additional action discussed above would ordinarily be taken, such as a warning on terminal screens, entry

in master logs, and the like. The operation of device 10 just described is closed loop in that a response, or lack thereof, from central processing unit 16 back to device 10 is involved in the operation.

If the violation frequency is greater than the threshold provided in step 120 but less than some higher threshold C, as determined in step 122 shown in the flow chart of Fig. 4, receiver-transmitter 72 and controller 60 operate interrupt device 70 that acts directly on central processing unit 16 to disable the program, as at step 124. Receiver-transmitter 72 and controller 60 also operates interrupt device 58 to send a disable message directly from device 10 to terminal 14, as at step 129. This is a Level III violation.

For Level III violations, operation of the computer system can only be restored or released by the insertion of a key sequence from computer terminal 14 to controller 60 or cartridge 82 as at step 126. This could be done by the user's supervisory personnel. Or it could be done by a field service representative of the program supplier, either locally through user's terminal 14 or remote from terminal of the supplier connected by a modem.

It should be noted that, at violation Level III, the operation of protection device 10 does not depend on the application software in central processing unit 16. Rather, protection device 10 operates independently on central processing unit 16 to disable operation of the protected software.

For very, very frequent violations greater than frequency C, that can only indicate deliberate attempts to secure unauthorized access to the program, protection device 10 again disables the program in the same manner as described in the preceding paragraph as at step 128. However, protection device 10 will only restore operation of the protected software by a key sequence inputted to controller 60 from the program supplier's factory, as through a modem connected either to central processing unit 16 or protective device 10 or from terminal 14, as at step 130. This is termed a Level IV violation.

Data relating to the number of unauthorized requests and the time they are occurring indicated at steps 114 and 116 in Fig. 4 may be used to assist in detecting the source of the unauthorized requests.

In a usual embodiment of software protection device 10, the typical data shown in the following data table would be provided in each cartridge 82. It is anticipated that each cartridge 82 could typically be of sufficient storage capacity for the data relating up to approximately one hundred software packages. The data table is as follows.

I. Cartridge Related Data
- A. Serial number of cartridge
- B. Cartridge modification count
- C. Cartridge Shipping date
- D. Last cartridge update
- E. Date that software authorization will terminate
- F. Date of warning of impending termination
- G. Run hours warning
- H. Cartridge maintenance data
  1. Access validation data (validates access to cartridge data)
  2. Modification validation data (validates modification)
- I. Warning messages text
- J. Owner of software license
- K. Software reseller No. 1
- L. Software reseller No. 2

II. Software Package related data.
- A. Identification of software package
- B. Authorization data
  1. Demonstration package?
  2. Non-demonstration package
     a. terminals allowed for this software package
     b. number of currently active terminals
     c. number of terminals authorized
- C. Detection data
  1. Criteria
     a. level required for warning
     b. level required for timed disable
     c. level required for terminal released disable
     d. level required for cpu released disable
  2. Occurrence data
     a. number of violations
     b. time of last violation
     c. moving average of frequency of violations

The foregoing data table provides the data necessary for operation of the protective system, as well as the necessary control information to the software supplier.

As will be noted from the data table, cartridges 82 may be reprogrammed from terminal 14 to alter the limits of authorization. For example, in return for increased payments, the limits of authorization can be expanded. Any such changes require proper validation and modification access data or passwords.

The application software may be transferred to another central processing unit by transferring both the software and protection device 10 or, at least the appropriate cartridge 82. However, if transfer of the software is attempted without the cartridge 82, the software cannot be made to run.

Fig. 5 shows a device 10A of the present invention suitable for use with a computer system

having only a single data line 12 for both data and security information. The configuration of device 10A generally resembles that of device 10 as shown in Fig. 2. Interrupt means 58 is connected in data signal line 12 to disable operation of the software and provide messages from receiver-transmitter 72 to the screen of terminal 14.

Fig. 6 shows a device 10B of the present invention suitable for operating solely through the associated additional peripheral port of central processing unit 16. All warning and interrupt messages are transmitted through this port of the central processing unit via the line 18.

Fig. 7 schematically shows use of a plurality of software protection devices 10-1, 10-2 and the associated interrupt devices 58 and 70 between terminal 14 and central processing unit 16. Protection devices 10-1 and 10-2 are connected in series on security line 18 and/or, if applicable, on data signal line 12. The use of additional protection devices 10 increases the number of software packages that can be protected.

Claims

1. Apparatus (10) for monitoring the use of software in a computer system with respect to at least one selected aspect of such use, the computer system having a central processor (16) containing the software, the central processor (16) being accessed by at least one operator terminal (14) connected to the central processor; the apparatus (10) comprising receiving means (72) coupled to the central processor (16), memory means (82) for containing data establishing the software usage limit for the selected aspect, microprocessor control means (60), and interrupt means (58,70); characterised in that the software in the central processor (16) generates usage data indicative of monitored software usage for the selected aspect of the computer system, the apparatus employing at least one pre-established level of occurrences of conditions violating the usage limit for the selected aspect when monitoring use of the software; in that the receiving means (72) is coupled to the central processor (16) for receiving the monitored software usage data from software in the central processor; in that the memory means (82) contains data establishing the pre-established level of occurrences of violating conditions, and stores violating condition occurrence data arising from operation of the computer system, and records data indicative of existing usage of the monitored software; in that the microprocessor control means (60) is coupled to the receiving means (72) and to the memory means (82) for determining, in response to the usage data, the conditions violating said usage limit and for determining whether the occurrence of the violating conditions bears a predetermined relationship to the established level of occurrences of violating conditions; and in that the interrupt means (58,70) is coupled to the computer system and to the control means (60), and is controlled by the control means to provide an output to the computer system when occurrences of violating conditions bear the predetermined relationship to the established level of occurrences of violating conditions, said output operating to control, in accordance with the relationship thus determined, the use of the software in the computer system in a predetermined manner.

2. Apparatus according to claim 1 for restricting the use of monitored software in a computer system in accordance with a usage limit established for a number of permitted concurrent usages of the monitored software, the central processor (16) being accessed by at least two operator terminals (14) connected to the central processor, wherein the memory means (82) contains data establishing the software usage limit for the number of concurrent usages of the monitored software and records data indicative of the concurrent usages of the monitored software.

3. Apparatus according to claim 1 or claim 2, wherein the interrupt means (58,70) provides an output to the computer system for restricting use of the monitored software.

4. Apparatus according to claim 2, wherein the concurrent use is evidenced by the number of operator terminals concurrently using the monitored software and wherein the apparatus restricts use of the monitored software in accordance with a usage limit established for the number of operator terminals (14) permitted to concurrently use the monitored software.

5. Apparatus according to any preceding claim, wherein the memory means (82) contains data establishing at least two violative condition occurrence levels.

6. Apparatus according to any of claims 1 to 4 further defined as employing at least two pre-established levels of occurences of conditions violative of the usage limit for the selected aspect, wherein the memory means (82) contains data establishing violative condition occurrence levels and wherein the control means

(60) is set to a first state that permits use of the monitored software in the central processor (16) or to a second state that restricts use of the monitored software, the control means (60) changing from the first state to the second state when the occurrence of violative conditions bears a predetermined relationship to a violative condition occurrence level, the control means (60) being capable of being reset from the second state to the first state by remotely generated resetting instructions, and wherein the interrupt means (58,70) provides an output to the computer system when the control means (60) is in the second state for restricting use of the monitored software.

7. Apparatus according to any preceding claim, wherein the control means (60) and interrupt means (58,70) provide a signal indicating improper usage requests to the software in the central processor (16) upon the existence of a first occurrence level.

8. Apparatus according to any preceding claim wherein the control means (60) and interrupt means (58,70) prevent the monitored software from operating in the central processor (16) upon the existance of a second occurrence level.

9. Apparatus according to any preceding claim, wherein the memory means (82) contains data establishing levels in the frequency of violative condition occurrences.

10. Apparatus according to claim 9, further comprising timing means in the control means (60) operable when the frequency of a violative condition occurence exceeds a predetermined level and requiring a timely response from the central processor (16) to avoid operating the interrupt means (58,70).

11. Apparatus according to claim 10, wherein the timing means have a predetermined timing interval, the timing means commencing a timing interval when the frequency of a violative condition occurrences exceeds a pre-established level, the control means (60) and interrupt means (58,70) providing a signal to the software in the central processor (16) indicating commencement of the timing interval and providing a signal preventing the monitored software from operating in the central processor (16) unless a response is received from the central processor within the timing interval of the timer.

12. Apparatus according to any of the preceding claims wherein the control means (60) is set to a first state that permits use of software in the central processor (16) or to a second state that restricts use of software, and wherein the control means (60) can be reset from the second state to the first state.

13. Apparatus according to any preceding claim, further including transmitter means coupled to the control means and to the interrupt means for transmitting warning signals generated by the control means to the central processor.

14. Apparatus according to any one of claims 1 to 12, wherein the interrupt means is coupled to at least one operator terminal, the apparatus further including transmitter means (72) coupled to the control means and to the interrupt means for transmitting warning signals generated by the control means to at least one of the the operator terminal and central processor.

15. Apparatus according to any preceding claim wherein the interrupt means (58,70) is coupled to the central processor (16) by means of a data signal link (12) and wherein the receiver means (72) is coupled to the data signal link (12).

16. Apparatus according to any one of claims 1 to 13, wherein the central processor of the computer system has a security signal link (18) and wherein the interrupt means (58,70) and receiver means are coupled to the security signal link (18) of the central processor (16).

17. Apparatus according to any one of claims 1 to 13, wherein the central processor (16) of the computer system has a security signal link (18) and has a data signal link (12), wherein the interrupt means includes means (58) coupled to the data signal link (12) and means (70) coupled to the security signal link (18), and wherein the receiving means is coupled to the security signal link.

18. Apparatus according to claim 16 or claim 17, wherein the transmitter means (72) are coupled to the security signal link.

19. Apparatus according to claim 18, wherein the transmitter means is connected to the data signal link.

20. Apparatus according to any preceding claim, wherein the memory means (82) is contained

in an element removable from the apparatus.

21. Apparatus according to any preceding claim, wherein the memory means (82) further comprises programmable memory means in which the data of the memory means may be altered.

22. Apparatus according to claim 21, wherein the memory means (82) comprises an EEPROM.

23. Apparatus according to any preceding claim, wherein the central processor (16) of the computer system has an operating system and wherein the apparatus further includes additional memory means (80) coupled to the control means containing data relating to the operating system of the central processor (16).

24. Apparatus according to claim 20, wherein the additional memory means (80) comprises an EEPROM.

25. Apparatus according to any preceding claim, wherein the receiving means and the interrupt means (72) include means for connecting an additional software use monitoring apparatus in series therewith, the apparatus further including a plurality of software monitoring apparatuses connected in series for monitoring additional software in the computer system.

Revendications

1. Dispositif (10) pour contrôler l'emploi d'un logiciel dans un système de traitement de l'information en ce qui concerne au moins un aspect sélectionné de cet emploi, le système de traitement de l'information comportant un processeur central (16) contenant le logiciel, l'accès étant fait au processeur central (16) par au moins un terminal d'opérateur (14) connecté au processeur central; le dispositif (10) comprenant un moyen récepteur (72) couplé au processeur central (16), un moyen à mémoire (82) pour contenir des données établissant la limite d'usage du logiciel pour l'aspect sélectionné, un moyen contrôleur à microprocesseur (60), et un moyen interrupteur (58,70); caractérisé en ce que le logiciel inclus dans le processeur central (16) génère des données d'usage indiquant un usage du logiciel contrôlé pour l'aspect sélectionné du système de traitement de l'information, le dispositif mettant en oeuvre au moins un niveau préétabli d'apparitions de conditions violant la limite d'usage pour l'aspect sélectionné pendant un contrôle de l'emploi du logiciel; en ce que le moyen récepteur (72) est couplé au processeur central (16) pour recevoir les données d'usage du logiciel contrôlé en provenance du logiciel inclus dans le processeur central; en ce que le moyen à mémoire (82) contient des données établissant le niveau préétabli d'apparitions de conditions de violation, et mémorise des données d'apparition de conditions de violation résultant du fonctionnement du système de traitement de l'information, et enregistre des données indiquant l'usage existant du logiciel contrôlé; en ce que le moyen contrôleur à microprocesseur (60) est couplé au moyen récepteur (72) et au moyen à mémoire (82) pour déterminer, en réponse aux données d'usage, les conditions violant ladite limite d'usage et pour déterminer si l'apparition des conditions de violation comporte un rapport prédéterminé vis-à-vis du niveau établi d'apparitions de conditions de violation; et en ce que le moyen interrupteur (58,70) est couplé au système de traitement de l'information et au moyen contrôleur (60), et est commandé par le moyen contrôleur pour fournir un signal de sortie au système de traitement de l'information quand les apparitions de conditions de violation comportent un rapport prédéterminé vis-à-vis du niveau établi d'apparitions de conditions de violation, ledit signal de sortie agissant pour commander, selon le rapport ainsi déterminé, l'emploi du logiciel dans le système de traitement de l'information d'une manière prédéterminée.

2. Dispositif selon la revendication 1, pour limiter l'emploi du logiciel contrôlé dans un système de traitement de l'information conformément à une limite d'usage établie pour un certain nombre d'usages concurrents admis du logiciel contrôlé, l'accès au processeur central (16) étant fait par au moins deux terminaux d'opérateur (14) connectés au processeur central, dans lequel le moyen à mémoire (82) contient des données établissant la limite d'usage du logiciel pour le nombre d'usages concurrents du logiciel contrôlé et enregistre des données indiquant les usages concurrents du logiciel contrôlé.

3. Dispositif selon l'une quelconque des revendications 1 et 2, dans lequel le moyen interrupteur (58,70) fournit un signal de sortie au système de traitement de l'information pour limiter l'emploi du logiciel contrôlé.

4. Dispositif selon la revendication 2, dans lequel l'emploi concurrent est mis en évidence par le nombre de terminaux d'opérateur employant en concurrence le logiciel contrôlé et dans

lequel le dispositif limite l'emploi du logiciel contrôlé conformément à une limite d'usage établie pour le nombre de terminaux d'opérateur (14) admis à employer en concurrence le logiciel contrôlé.

5. Dispositif selon l'une quelconque des revendications 1 à 4, dans lequel le moyen à mémoire (82) contient des données établissant au moins deux niveaux d'apparition de conditions de violation.

6. Dispositif selon l'une quelconque des revendications 1 à 4, défini en outre comme mettant en oeuvre au moins deux niveaux préétablis d'apparitions de conditions violant la limite d'usage pour l'aspect sélectionné, dans lequel le moyen à mémoire (82) contient des données établissant des niveaux d'apparition de conditions de violation et dans lequel le moyen contrôleur (60) est mis à un premier état qui permet l'emploi du logiciel contrôlé dans le processeur central (16) ou à un second état qui limite l'emploi du logiciel contrôlé, le moyen contrôleur (60) passant du premier état au second état quand l'apparition de conditions de violation comporte un rapport prédéterminé vis-à-vis d'un niveau d'apparition de conditions de violation, le moyen contrôleur (60) pouvant être remis du second état au premier état par des instructions de remise à l'état initial générées à distance, et dans lequel le moyen interrupteur (58,70) fournit un signal de sortie au système de traitement de l'information quand le moyen contrôleur (60) est dans le second état pour limiter l'emploi du logiciel contrôlé.

7. Dispositif selon l'une quelconque des revendications 1 à 6, dans lequel le moyen contrôleur (60) et le moyen interrupteur (58,70) fournissent un signal indiquant des demandes d'usage incorrectes au logiciel inclus dans le processeur central (16) au cours de l'existence d'un premier niveau d'apparition.

8. Dispositif selon l'une quelconque des revendications 1 à 7, dans lequel le moyen contrôleur (60) et le moyen interrupteur (58,70) empêchent le logiciel contrôlé d'agir dans le processeur central (16) au cours de l'existence d'un deuxième niveau d'apparition.

9. Dispositif selon l'une quelconque des revendications 1 à 8, dans lequel le moyen à mémoire (82) contient des données établissant des niveaux dans la fréquence des apparitions de conditions de violation.

10. Dispositif selon la revendication 9, comprenant en outre un moyen de synchronisation dans le moyen contrôleur (60) pouvant fonctionner quand la fréquence d'apparition de conditions de violation dépasse un niveau prédéterminé et exigeant une réponse synchronisée du processeur central (16) pour éviter le fonctionnement du moyen interrupteur (58,70).

11. Dispositif selon la revendication 10, dans lequel le moyen de synchronisation comporte un intervalle de synchronisation prédéterminé, le moyen de synchronisation commençant un intervalle de synchronisation quand la fréquence d'apparition des conditions de violation dépasse un niveau préétabli, le moyen contrôleur (60) et le moyen interrupteur (58,70) fournissant un signal au logiciel inclus dans le processeur central (16) indiquant le commencement de l'intervalle de synchronisation et fournissant un signal empêchant le logiciel contrôlé d'agir dans le processeur central (16) à moins qu'une réponse soit reçue du processeur central dans l'intervalle de synchronisation du moyen de synchronisation.

12. Dispositif selon l'une quelconque des revendications 1 à 11, dans lequel le moyen contrôleur (60) est mis à un premier état qui permet l'emploi du logiciel dans le processeur central (16) ou à un second état qui limite l'emploi du logiciel, et dans lequel le moyen contrôleur (60) peut être remis du second état au premier état.

13. Dispositif selon l'une quelconque des revendications 1 à 12, incluant en outre un moyen émetteur couplé au moyen contrôleur et au moyen interrupteur pour émettre des signaux d'avertissement engendrés par le moyen contrôleur vers le processeur central.

14. Dispositif selon l'une quelconque des revendications 1 à 12, dans lequel le moyen interrupteur est couplé à au moins un terminal d'opérateur, le dispositif incluant en outre un moyen émetteur (72) couplé au moyen contrôleur et au moyen interrupteur pour émettre des signaux d'avertissement engendrés par le moyen contrôleur vers au moins un du terminal d'opérateur et du processeur central.

15. Dispositif selon l'une quelconque des revendications 1 à 14, dans lequel le moyen interrupteur (58,70) est couplé au processeur central (16) au moyen d'une liaison pour signaux de données (12) et dans lequel le moyen récepteur (72) est couplé à la liaison pous signaux

de données (12).

16. Dispositif selon l'une quelconque des revendications 1 à 13, dans lequel le processeur central du système de traitement de l'information comporte une liaison pour signaux de sécurité (18) et dans lequel le moyen interrupteur (58,70) et le moyen récepteur sont couplés à la liaison pour signaux de sécurité (18) du processeur central (16).

17. Dispositif selon l'une quelconque des revendications 1 à 13, dans lequel le processeur central (16) du système de traitement de l'information comporte une liaison pour signaux de sécurité (18) et comporte une liaison pour signaux de données (12), dans lequel le moyen interrupteur comprend un moyen (58) couplé à la liaison pour signaux de données (12) et un moyen (70) couplé à la liaison pour signaux de sécurité (18), et dans lequel le moyen récepteur est couplé à la liaison pour signaux de sécurité.

18. Dispositif selon l'une quelconque des revendications 16 et 17, dans lequel le moyen émetteur (72) est couplé à la liaison pour signaux de sécurité.

19. Dispositif selon la revendication 18, dans lequel le moyen émetteur est connecté à la liaison pour signaux de données.

20. Dispositif selon l'une quelconque des revendications 1 à 19, dans lequel le moyen à mémoire (82) est contenu dans un élément amovible du dispositif.

21. Dispositif selon l'une quelconque des revendications 1 à 20, dans lequel le moyen à mémoire (82) comprend en outre un moyen à mémoire programmable dans lequel les données du moyen à mémoire peuvent être modifiées.

22. Dispositif selon la revendication 21, dans lequel le moyen à mémoire (82) comprend une mémoire morte programmable effaçable électriquement (EEPROM).

23. Dispositif selon l'une quelconque des revendications 1 à 22, dans lequel le processeur central (16) du système de traitement de l'information comporte un système d'exploitation et dans lequel le dispositif inclut en outre un moyen à mémoire supplémentaire (80) couplé au moyen contrôleur contenant des données relatives au système d'exploitation du processeur central (16).

24. Dispositif selon la revendication 20, dans lequel le moyen à mémoire supplémentaire (80) comprend une mémoire EEPROM.

25. Dispositif selon l'une quelconque des revendications 1 à 24, dans lequel le moyen récepteur et le moyen interrupteur (72) comprennent des moyens pour connecter un dispositif de contrôle de l'emploi d'un logiciel supplémentaire en série avec ceux-ci, le dispositif incluant en outre un ensemble de dispositifs de contrôle de logiciel connectés en série pour contrôler le logiciel supplémentaire dans le système de traitement de l'information.

Patentansprüche

1. Vorrichtung (10) zum Überprüfen der Verwendung einer Software in einem Computersystem bezüglich wenigstens einem ausgewählten Verwendungsaspekt, wobei das Computersystem einen Zentralprozessor (16) mit der Software aufweist sowie mindestens eine mit dem Zentralprozessor verbundene Bedienungs-Datenstation (14), die zugriff auf den Zentralprozessor hat, und wobei die Vorrichtung (10) ein mit dem Zentralprozessor (16) verbundenes Empfangsmittel (72) hat, ein Speichermittel (82), das Daten, die die Software-Verwendungsgrenze für den ausgewählten Aspekt begründen, enthält sowie ein Mikroprozessor-Steuermittel (60) und ein Unterbrechungsmittel (58, 70), dadurch gekennzeichnet, daß die Software in dem Zentralprozessor (16) Verwendungsdaten erzeugt, die für die überprüfte Software-Verwendung für den ausgewählten Aspekt des Computersystems bezeichnend sind, wobei die Vorrichtung, wenn die Verwendung der Software überprüft wird, wenigstens ein voreingestelltes Niveau von Vorkommen von Bedingungen benutzt, die die Verwendungsgrenze für den ausgewählten Aspekt verletzen; daß das Empfangsmittel (72) mit dem Zentralprozessor (16) verbunden ist zum Empfang der überprüften Software-Verwendungsdaten von der Software in den Zentralprozessor; daß das Speichermittel (82) Daten enthält, die das voreingestellte Niveau von Vorkommen von verletzenden Bedingungen etablieren, und das Speichermittel die verletzenden Bedingungsvorkommen-Daten, die mit dem Betrieb des Computersystems entstehen, speichert sowie die Daten abspeichert, die für die bestehende Verwendung der überprüften Software bezeichnend sind; daß das Mikroprozessor-Steuermittel (60) mit dem

Empfangsmittel (72) und dem Speichermittel (82) verbunden ist, um in Reaktion auf die Verwendungsdaten die Bedingungen zu bestimmen, die die Verwendungsgrenze verletzen, und zur Bestimmung, ob das Vorkommen der verletzenden Bedingungen einen Bezug hat auf eine vorbestimmte Beziehung zu dem aufgestellten Niveau von Vorkommen von verletzenden Bedingungen; und daß das Unterbrechungsmittel (58, 70) mit dem Computersystem und dem Steuermittel (60) verbunden ist und von dem Steuermittel gesteuert wird, um eine Ausgabe an das Computersystem zu schaffen, wenn die Vorkommen der verletzenden Bedingungen einen Bezug haben auf die vorbestimmte Beziehung zu dem aufgestellten Niveau der Vorkommen von verletzenden Bedingungen, wobei die Ausgabe so arbeitet, daß gemäß der so bestimmten Beziehung die Verwendung der Software in dem Computersystem in einer vorbestimmten Weise gesteuert wird.

2. Vorrichtung nach Anspruch 1 für die Einschränkung der Verwendung der überprüften Software in einem Computersystem entsprechend einer Verwendungsgrenze, die für eine Anzahl von erlaubten, gleichzeitigen Verwendungen der überprüften Software errichtet ist, wobei auf den Zentralprozessor (16) wenigstens zwei Bedienungs-Datenstationen (14) Zugriff haben, worin das Speichermittel (82) Daten enthält, die die Software-Verwendungsgrenze für eine Anzahl von gleichzeitigen Verwendungen der überprüften Software begründen, und Daten speichert, die für die gleichzeitigen Verwendungen der überprüften Software bezeichnend sind.

3. Vorrichtung nach Anspruch 1 oder Anspruch 2, worin das Unterbrechungsmittel (58, 70) eine Ausgabe an das Computersystem schafft, um die Verwendung der überprüften Software zu beschränken.

4. Vorrichtung nach Anspruch 2, worin die gleichzeitige Verwendung an der Zahl der Bedienungs-Datenstationen erkennbar ist, die gleichzeitig die überprüfte Software benutzen, und worin die Vorrichtung die Verwendung der überprüften Software beschränkt gemäß einer Verwendungsgrenze, die für die Zahl der Bedienungs-Datenstationen (14) errichtet ist, welche gleichzeitig die überprüfte Software benutzen dürfen.

5. Vorrichtung nach einem der vorangehenden Ansprüche, worin das Speichermittel (82) Daten enthält, die wenigstens zwei Niveaus von verletzenden Bedingungsvorkommen begründen.

6. Vorrichtung nach einem der Ansprüche 1 bis 4 und ferner definiert durch die Verwendung von wenigstens zwei voreingestellten Niveaus von Vorkommen von Bedingungen, die die Verwendungsgrenze für den ausgewählten Aspekt verletzen, worin das Speichermittel (82) Daten enthält, die Niveaus von verletzenden Bedingungsvorkommen begründen, und worin das Speichermittel (60) auf einen ersten Zustand eingestellt ist, der die Verwendung der überprüften Software in dem Zentralprozessor (16) erlaubt, oder auf einen zweiten Zustand, der die Verwendung der überprüften Software beschränkt, wobei die Steuervorrichtung (60) von dem ersten in den zweiten Zustand wechselt, wenn das Vorkommen von verletzenden Bedingungen einen Bezug hat auf eine vorbestimmte Beziehung zu einem Niveau von verletzenden Bedingungsvorkommen, und das Steuermittel (60) von dem zweiten Zustand in den ersten Zustand durch fernerzeugte Rücksetzinstruktionen zurückversetzt werden kann, und worin das Unterbrechungsmittel (58, 70) eine Ausgabe an das Computersystem schafft, wenn das Steuermittel (60) in dem zweiten Zustand ist zur Beschränkung der Verwendung der überprüften Software.

7. Vorrichtung nach einem der vorangehenden Ansprüche, worin das Steuermittel (60) und das Unterbrechungsmittel (58, 70) bei Vorliegen eines ersten Vorkommenniveaus ein Signal schafft, das eine falsche Verwendungsanfrage an die Software in dem Zentralprozessor (16) anzeigt.

8. Vorrichtung nach einem der vorangehenden Ansprüche, worin das Steuermittel (60) und das Unterbrechungsmittel (58, 70) bei Vorliegen eines zweiten Vorkommenniveaus die überprüfte Software daran hindert in dem Zentralprozessor (16) zu arbeiten.

9. Vorrichtung nach einem der vorangehenden Ansprüche, worin das Speichermittel (82) Daten enthält, die Niveaus in der Frequenz von verletzenden Bedingungsvorkommen begründen.

10. Vorrichtung nach Anspruch 9, die ferner in dem Steuermittel (60) ein Zeitmittel aufweist, das betriebsfähig ist, wenn die Frequenz eines verletzenden Bedingungsvorkommens ein vorbestimmtes Niveau überschreitet, und die eine

Zeitantwort aus dem Zentralprozessor (16) benötigt, um den Betrieb des Unterbrechungsmittels (58, 70) zu vermeiden.

11. Vorrichtung nach Anspruch 10, worin das Zeitmittel ein vorbestimmtes Zeitintervall hat, wobei das Zeitmittel ein Zeitintervall startet, wenn die Frequenz von verletzenden Bedingungsvorkommen ein vorbestimmtes Niveau überschreitet, wobei das Steuermittel (60) und das Unterbrechungsmittel (58, 70) ein Signal an die Software in dem Zentralprozessor (16) bereitstellt, das den Start des Zeitintervalls anzeigt, und ein Signal schafft, das den Betrieb der überprüften Software in dem Zentralprozessor (16) verhindert bis eine Antwort von dem Zentralprozessor innerhalb des Zeitintervalls des Zeitgebers empfangen wird.

12. Vorrichtung nach einem der vorangehenden Ansprüche, worin das Steuermittel (60) auf einen ersten Zustand eingestellt ist, der die Verwendung der Software in dem Zentralprozessor (16) erlaubt, oder auf einen zweiten Zustand, der die Verwendung der Software beschränkt, und worin das Steuermittel (60) von dem zweiten Zustand in den ersten Zustand zurückgestellt werden kann.

13. Vorrichtung nach einem der vorangehenden Ansprüche, die ferner ein Sendemittel aufweist, das mit dem Steuermittel und dem Unterbrechungsmittel verbunden ist für die Übersendung von Warnsignalen, die von dem Steuermittel erzeugt werden, an den Zentralprozessor.

14. Vorrichtung nach einem der Ansprüche 1 bis 12, worin das Unterbrechungsmittel mit wenigstens einer Bedienungs-Datenstation verbunden ist, wobei die Vorrichtung ferner ein Sendemittel (72) aufweist, das mit dem Steuermittel und dem Unterbrechungsmittel verbunden ist für die Übermittlung von Warnsignalen, die von dem Steuermittel erzeugt werden, an wenigstens einen der Bedienungs-Datenstationen und den Zentralprozessor.

15. Vorrichtung nach einem der vorangehenden Ansprüche, worin das Unterbrechungsmittel (58, 70) durch eine Datensignalverbindung (12) mit dem Zentralprozessor (16) verbunden ist, und worin das Empfangsmittel (72) mit der Datensignalverbindung (12) verbunden ist.

16. Vorrichtung nach einem der Ansprüche 1 bis 13, worin der Zentralprozessor des Computersystems eine Sicherheitssignalverbindung (18) hat, und worin das Unterbrechungsmittel (58, 70) und das Empfangsmittel mit der Sicherheitssignalverbindung (18) des Zentralprozessors (16) verbunden sind.

17. Vorrichtung nach einem der Ansprüche 1 bis 13, worin der Zentralprozessor (16) des Computersystems eine Sicherheitssignalverbindung (18) und eine Datensignalverbindung (12) hat, worin das Unterbrechungsmittel ein Mittel (58), das mit der Datensignalverbindung (12) verbunden ist, und ein Mittel (70), das mit der Sicherheitssignalverbindung (18) verbunden ist, aufweist, und worin das Empfangsmittel mit der Sicherheitssignalverbindung verbunden ist.

18. Vorrichtung nach Anspruch 16 oder Anspruch 17, worin das Sendemittel (72) mit der Sicherheitssignalverbindung verbunden ist.

19. Vorrichtung nach Anspruch 18, worin das Sendemittel mit der Datensignalverbindung verbunden ist.

20. Vorrichtung nach einem der vorangehenden Ansprüche, worin das Speichermittel (82) in einem Element angeordnet ist, das aus der Vorrichtung entfernbar ist.

21. Vorrichtung nach einem der vorangehenden Ansprüche, worin das Speichermittel (82) ferner ein programmierbares Speichermittel aufweist, in dem die Daten des Speichermittels geändert werden können.

22. Vorrichtung nach Anspruch 21, worin das Speichermittel (82) einen EEPROM aufweist.

23. Vorrichtung nach einem der vorangehenden Ansprüche, worin der Zentralprozessor (16) des Computersystems ein Betriebssystem hat, und worin die Vorrichtung ferner ein zusätzliches Speichermittel (80) aufweist, das mit dem Steuermittel verbunden ist und Daten bezüglich des Betriebssystems des Zentralprozessors (16) enthält.

24. Vorrichtung nach Anspruch 20, worin das zusätzliche Speichermittel (80) einen EEPROM aufweist.

25. Vorrichtung nach einem der vorangehenden Ansprüche, worin das Empfangsmittel und das Unterbrechungsmittel (72) ein Mittel aufweisen, um eine zusätzliche Softwareverwendungs-Überprüfungsvorrichtung damit in Serie zu schalten, wobei die Vorrichtung ferner mehrere Software-Uberprüfungsvorrichtungen aufweist,

die in Serie geschaltet sind, für die Überprüfung von zusätzlicher Software in dem Computersystem.

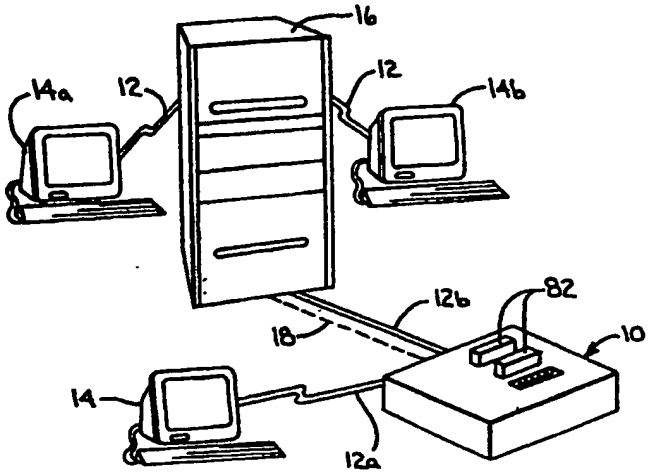

FIG. 1

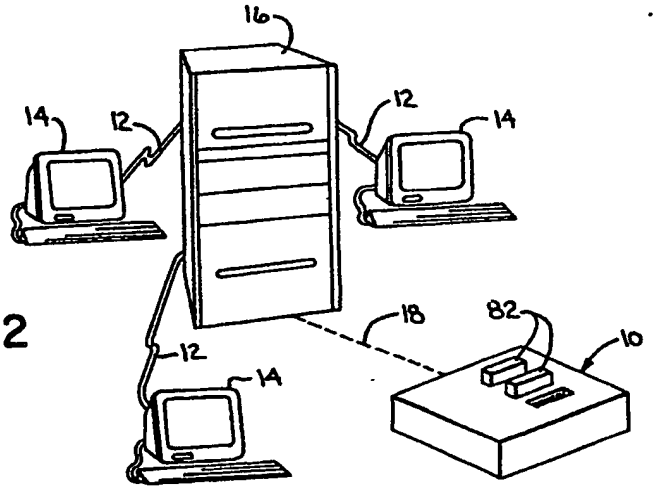

FIG.2

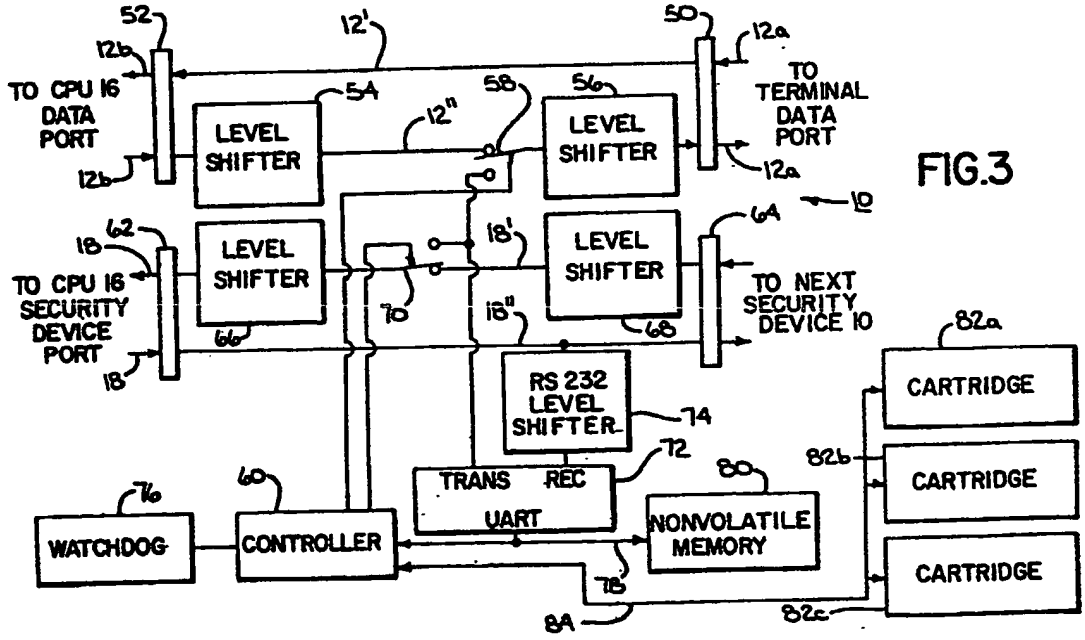

FIG.3

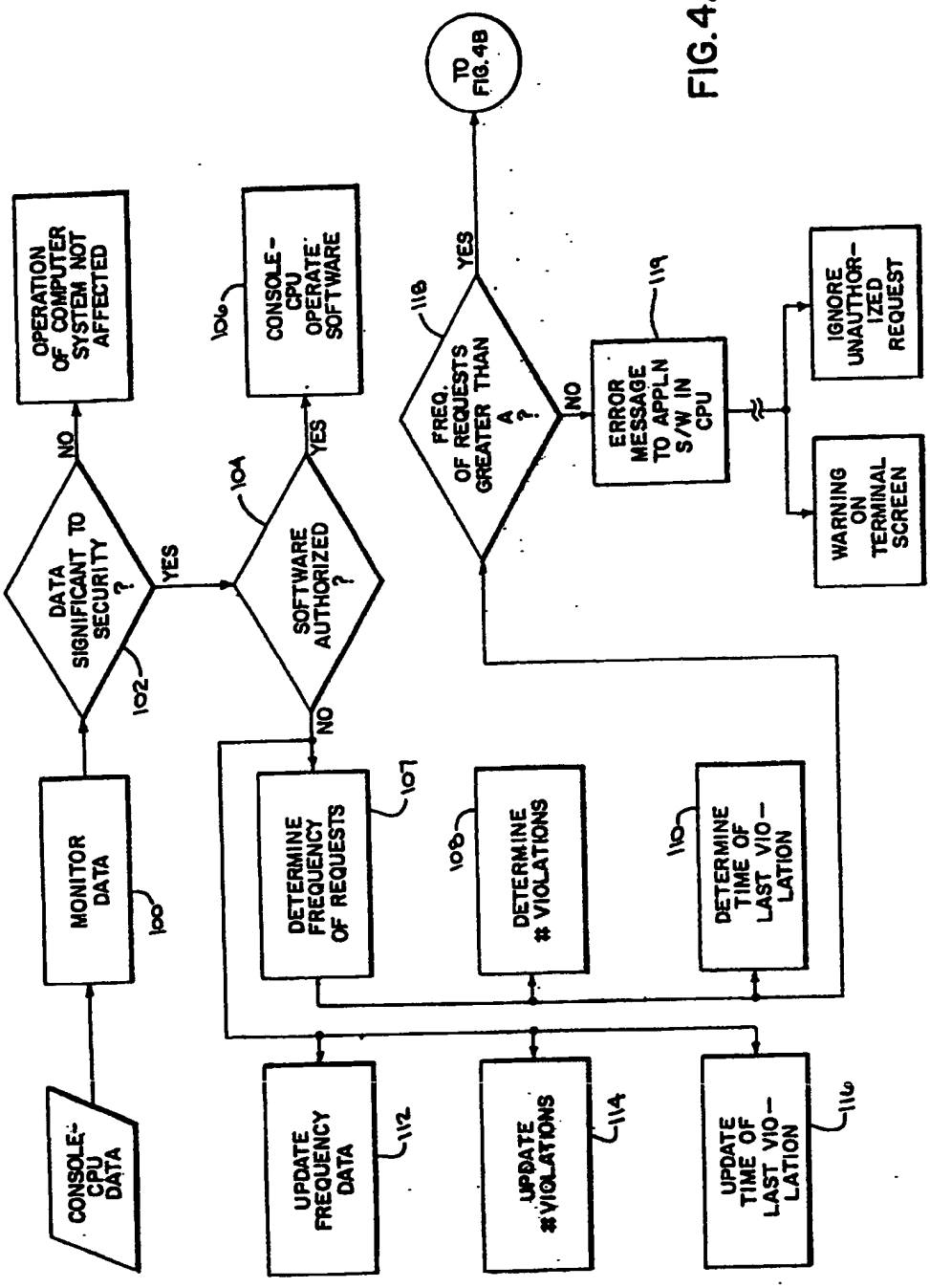
CONSOLE-CPU DATA
MONITOR DATA
100
DATA SIGNIFICANT TO SECURITY ?
102
NO
YES
OPERATION OF COMPUTER SYSTEM NOT AFFECTED
SOFTWARE AUTHORIZED ?
104
YES
NO
CONSOLE-CPU OPERATE SOFTWARE
106
DETERMINE FREQUENCY OF REQUESTS
107
DETERMINE # VIOLATIONS
108
DETERMINE TIME OF LAST VIO-LATION
110
UPDATE FREQUENCY DATA
112
UPDATE #VIOLATIONS
114
UPDATE TIME OF LAST VIO-LATION
116
FREQ. OF REQUESTS GREATER THAN A ?
118
YES
NO
TO FIG.4B
ERROR MESSAGE TO APPLN S/W IN CPU
119
IGNORE UNAUTHOR-IZED REQUEST
WARNING ON TERMINAL SCREEN

FIG.4A

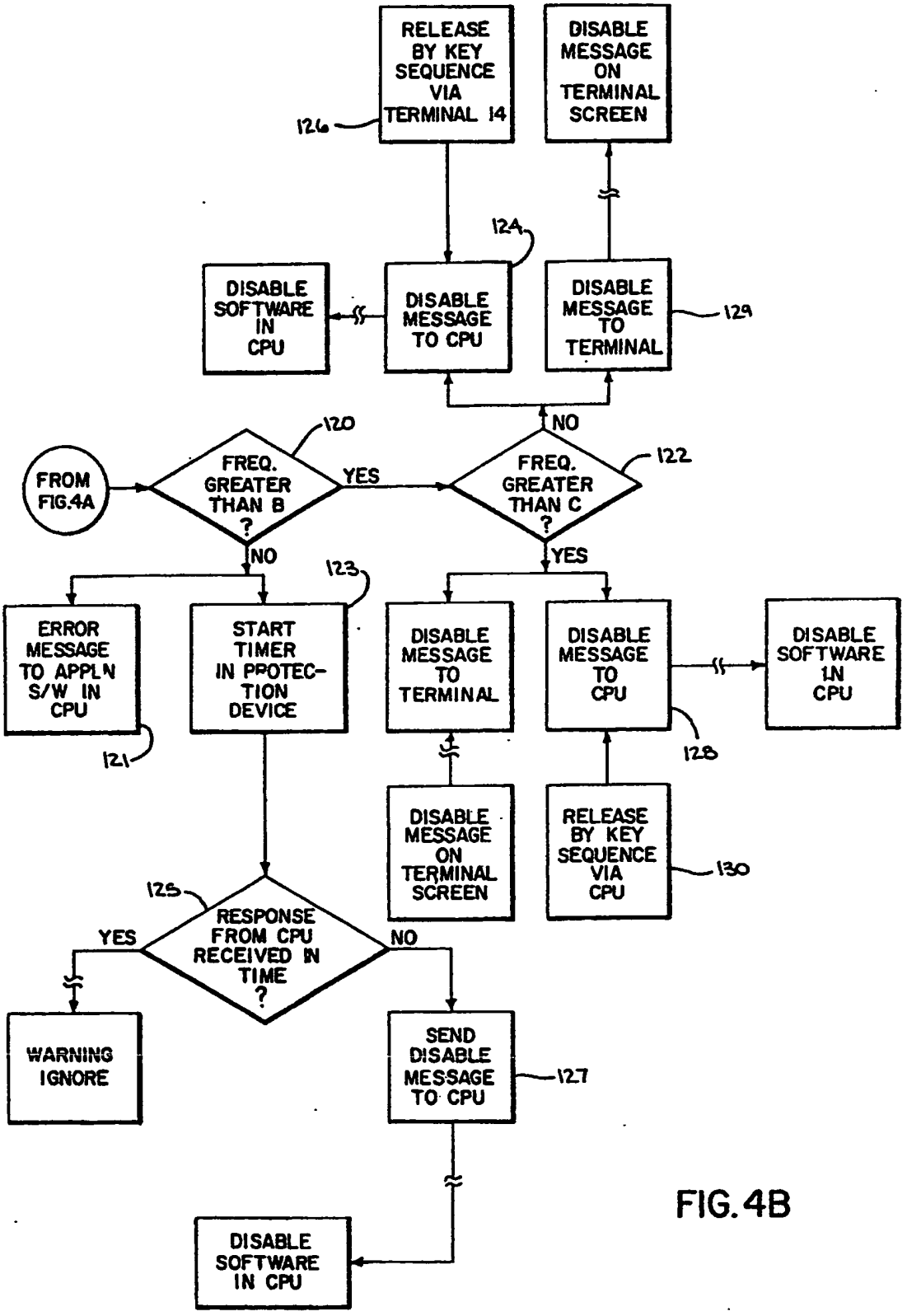
RELEASE BY KEY SEQUENCE VIA TERMINAL 14
126
DISABLE MESSAGE ON TERMINAL SCREEN
124
DISABLE SOFTWARE IN CPU
DISABLE MESSAGE TO CPU
DISABLE MESSAGE TO TERMINAL
129
NO
120
FROM FIG.4A
FREQ. GREATER THAN B ?
YES
FREQ. GREATER THAN C ?
122
NO
YES
123
ERROR MESSAGE TO APPLN S/W IN CPU
121
START TIMER IN PROTEC-TION DEVICE
DISABLE MESSAGE TO TERMINAL
DISABLE MESSAGE TO CPU
DISABLE SOFTWARE IN CPU
128
DISABLE MESSAGE ON TERMINAL SCREEN
RELEASE BY KEY SEQUENCE VIA CPU
130
125
RESPONSE FROM CPU RECEIVED IN TIME ?
YES
NO
WARNING IGNORE
SEND DISABLE MESSAGE TO CPU
127
DISABLE SOFTWARE IN CPU

FIG.4B

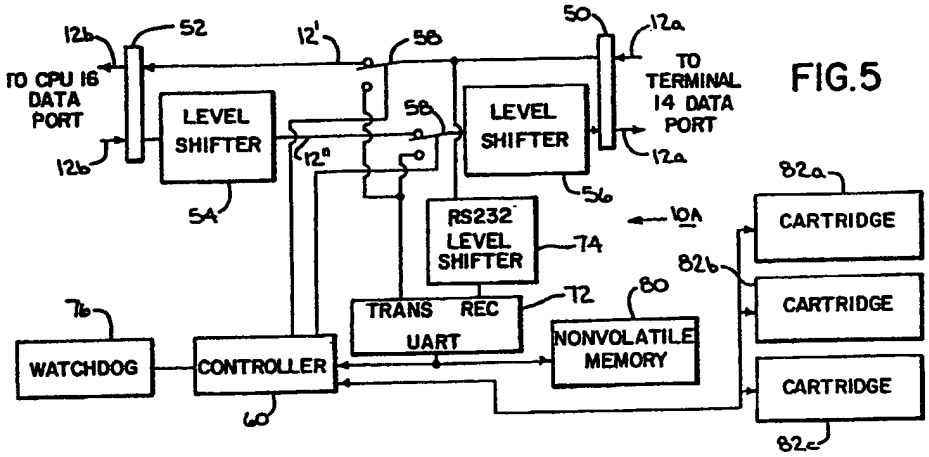

FIG.5

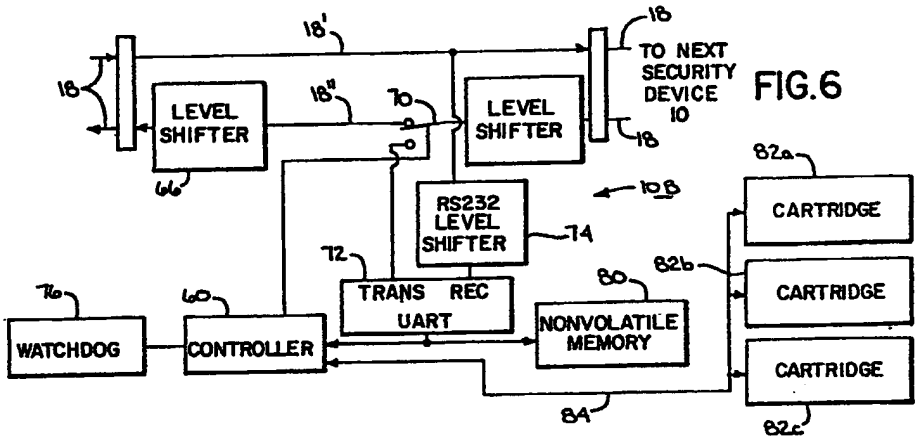

FIG.6

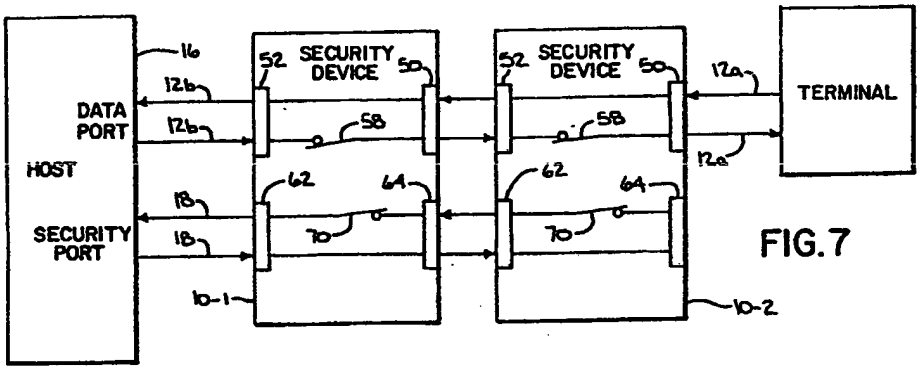

FIG.7